

REMARKS

As a preliminary matter, the Examiner has objected to Claim 21 because of an informality. Applicant has amended Claim 21 to correct this informality. Accordingly, Applicant respectfully asserts that Claim 21 is now in acceptable form. Therefore, Applicant respectfully requests Examiner remove the objection to Claim 21 because of various informalities.

The Examiner has rejected claims 22, 27, 31, 39, and 41, under 35 U.S.C. § 112, second paragraph, as being indefinite. The Examiner has also rejected claims 21-45 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,451,740 to Olgaard et al. ("Olgaard"). Claims 21-45 stand currently amended. Claim 48 stands newly added. Claims 1-20 stand previously canceled. Claims 46 and 47 stand previously withdrawn. Claims 21-48 are currently pending. The following remarks are considered by applicant to overcome each of the Examiner's outstanding rejections to current claims 21-45 and 48. An early Notice of Allowance is therefore requested.

I. THE NEXT ACTION CANNOT BE MARKED FINAL

As an initial matter, Applicant notes that, as a result of newly added Claim 48, the next Action cannot be marked as final.

II. SUMMARY OF RELEVANT LAW

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.

III. REJECTION OF CLAIMS 22, 27, 31, 39, AND 41 UNDER 35 U.S.C. § 112, SECOND PARAGRAPH, AS BEING INDEFINITE

On page 3 of the current Office Action, the Examiner rejects claims 22, 27, 31, 39, and 41 under 35 U.S.C. § 112, second paragraph, as being indefinite. These rejections are respectfully traversed and believed overcome in view of the following discussion.

In particular, Examiner asserts that certain phrases in claims 22, 31, 39, and 41 lack antecedent basis. Applicant has currently amended claims 22, 31, 39, and 41 so as to correct these deficiencies. Accordingly, Applicant respectfully asserts that claims 22, 31, 39, and 41 are now in acceptable form.

In addition, regarding Claim 27, Examiner asserts that it is unclear how a device such as the host system can be a conceptual entity such as a VPN. A virtual private network ("VPN") is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) as opposed to running across a single private network. See "Virtual private network." *Wikipedia, The Free Encyclopedia*. 28 Mar 2009, 15:47 UTC. 30 Mar 2009
<http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=280229248> (a copy of which is enclosed herewith in Appendix A). Since a virtual private network is an actual computer network, it clearly can act as a host system, as stated in Claim 27. Accordingly, Applicant respectfully asserts that Claim 27 is in acceptable form.

Therefore, Applicant respectfully requests Examiner remove the rejections of claims 22, 27, 31, 39, and 41 under 35 U.S.C. § 112, second paragraph, as being indefinite.

IV. REJECTION OF CLAIMS 21-45 UNDER 35 U.S.C. § 102(E) BASED ON OLGAARD

On page 3 of the current Office Action, the Examiner rejects claims 21-45 under 35 U.S.C. § 102(e) as being anticipated by Olgaard. These rejections are respectfully traversed and believed overcome in view of the following discussion.

Claim 21 states, in part:

“connecting the client system to the target network via a host system via a host system controlled by the software provided in the client system, wherein the step of connecting the client system to the target network comprises the steps of:

locating the target network through the host system;

determining requirements for connecting the client system to the target network; and

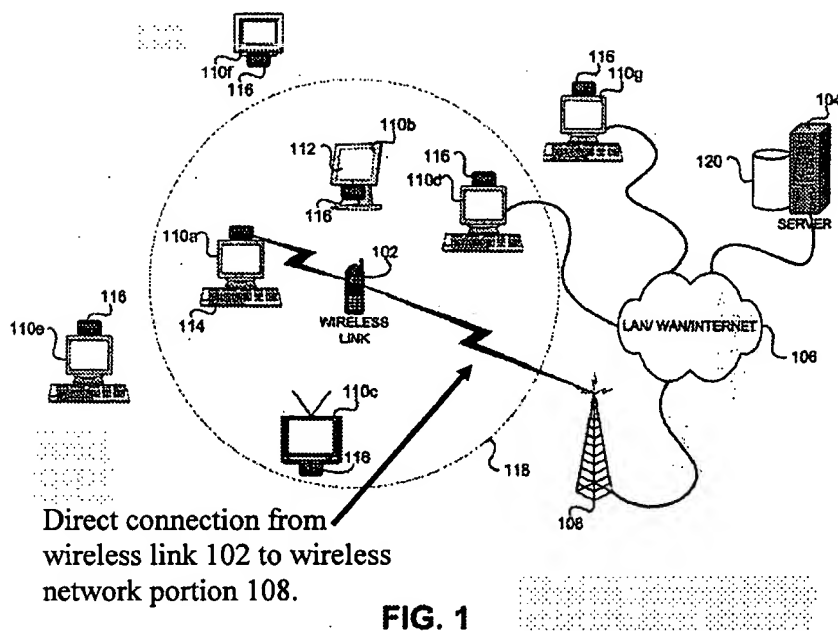
linking the client system to the target network based on the requirements....”

As such, Claim 21 states that the client system is connected to the target network via a host system, and that the target network is located through the host system. Examiner asserts that Olgaard discloses the above claim language. This, however, misinterprets the teachings of Olgaard.

More specifically, Olgaard teaches:

“A system, method and article of manufacture are provided for utilizing a wireless link in an interface roaming network. A wireless link is utilized to scan a vicinity of the wireless link to detect one or more interface clients in the vicinity. The wireless link then transmits to an infrastructure server information relating to the interface clients detected in the vicinity. Based on the transmitted information, the infrastructure server then selects one of the interface clients. Subsequently, the wireless link receives a notification from the infrastructure server of the selected interface client and a connection between the infrastructure server and the selected interface client is initiated for communication therebetween.” Olgaard, Col. 1, Lns. 31-43 (emphasis added).

As such, Olgaard teaches that a wireless link 102 (the closest disclosure to a “client system” in Olgaard) directly connects to a network 106 (the closest disclosure to a “target network” in Olgaard), which includes a wireless network portion 108. See Olgaard, Col. 4, Lns. This is seen clearly in the annotated version of Fig. 1 of Olgaard below:



As such, Olgaard teaches a direct connection between a wireless link 102 and wireless network portion 108, and not “connecting the client system to the target network via a host system via a host system” or “locating the target network through the host system”, as stated in Claim 21.

In addition, even if interface client 110a could be considered a client system (which Examiner does not assert and Applicant disputes), Olgaard would still fail to disclose the language of Claim 21. In particular, Olgaard teaches that the infrastructure server 104 locates and selects an interface client 110 through the network 106/108. Olgaard, Col. 1, Lns. 31-43; Col. 4, Lns. 543-67; Fig. 2, Steps 202 and 204. As such, Olgaard not only teaches that an interface client 110 is located as opposed to a network, but Olgaard also teaches that an interface client 110 is located through a network, as opposed to locating a network through a host system. As such, even if the interface client 110a could be considered a client system (which Examiner does not assert and Applicant disputes), Olgaard fails to teach the above language of Claim 21.

Moreover, a similar result is reached even if the infrastructure server 104 could be considered a client system (which Examiner does not assert and Applicant disputes). This is

because Olgaard teaches that the infrastructure server 104 connects directly to the network 106. Olgaard, Fig. 1. As such, the infrastructure server 104 does not connect to a target network via a host system as stated in Claim 21. Also, as stated above, Olgaard not only teaches that an interface client 110 is located as opposed to a network, but Olgaard also teaches that an interface client 110 is located through a network, as opposed to locating a network through a host system. As such, even if the infrastructure server 104 could be considered a client system (which Examiner does not assert and Applicant disputes), Olgaard fails to teach the above language of Claim 21.

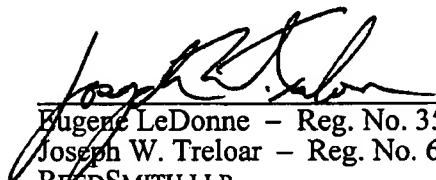
Accordingly, Applicant respectfully asserts that Examiner has failed to establish a prima facie case of anticipation of independent Claim 21, and corresponding claims 22-45 because they are ultimately dependant from independent Claim 21. Therefore, Applicants respectfully requests that Examiner remove the rejection of claims 21-45 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,451,740 to Olgaard et al.

V. NEW CLAIM 48

New Claim 48 depends from independent Claim 21. As Claim 21 is allowable, so must be Claim 48. Accordingly, Applicant respectfully asserts that Claim 48 is allowable. Therefore, Applicant respectfully requests Examiner allow Claim 48.

Based upon the above remarks, Applicant respectfully requests reconsideration of this application and its early allowance. Should the Examiner feel that a telephone conference with Applicant's attorney would expedite the prosecution of this application, the Examiner is urged to contact him at the number indicated below.

Respectfully submitted,



Eugene LeDonne - Reg. No. 35,930
Joseph W. Treloar - Reg. No. 60,975
REEDSMITH LLP
599 Lexington Avenue
New York, NY 10022
Tel.: 212.521.5400

EL:JWT

500836.20001

Appendix A

Virtual private network

From Wikipedia, the free encyclopedia

A **virtual private network (VPN)** is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) as opposed to running across a single private network. The link-layer protocols of the virtual network are said to be tunneled through the larger network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN service providers may offer best-effort performance, or may have a defined service level agreement (SLA) with their VPN customers. Generally, a VPN has a topology more complex than point-to-point.

A VPN allows computer users to access a network via an IP address other than the one that actually connects their computer to the Internet.

Contents

- 1 Categorization by user administrative relationships
- 2 Routing
 - 2.1 Building blocks
- 3 User-visible PPVPN services
 - 3.1 Layer 1 services
 - 3.1.1 Virtual private wire and private line services (VPWS and VPLS)
 - 3.2 Layer 2 services
 - 3.2.1 Virtual LAN
 - 3.2.2 Virtual private LAN service (VPLS)
 - 3.2.3 Pseudo wire (PW)
 - 3.2.4 IP-only LAN-like service (IPLS)
 - 3.3 L3 PPVPN architectures
 - 3.3.1 BGP/MPLS PPVPN
 - 3.3.2 Virtual router PPVPN
- 4 Categorizing VPN security models
 - 4.1 Authentication before VPN connection
 - 4.2 Trusted delivery networks
 - 4.3 Security mechanisms
 - 4.4 Security and mobility
- 5 See also
- 6 References
- 7 External links

Categorization by user administrative relationships

The Internet Engineering Task Force (IETF) has categorized a variety of VPNs, some of which, such as Virtual LANs (VLAN) are the standardization responsibility of other organizations, such as the Institute

of Electrical and Electronics Engineers (IEEE) Project 802, Workgroup 802.1 (architecture). Originally, Wide Area Network (WAN) links from a telecommunications service provider interconnected network nodes within a single enterprise. With the advent of LANs, enterprises could interconnect their nodes with links that they owned. While the original WANs used dedicated lines and layer 2 multiplexed services such as Frame Relay, IP-based layer 3 networks, such as the ARPANET, Internet, military IP networks (NIPRNET, SIPRNET, JWICS, etc.), became common interconnection media. VPNs began to be defined over IP networks ^[1]. The military networks may themselves be implemented as VPNs on common transmission equipment, but with separate encryption and perhaps routers.

It became useful first to distinguish among different kinds of IP VPN based on the administrative relationships (rather than the technology) interconnecting the nodes. Once the relationships were defined, different technologies could be used, depending on requirements such as security and quality of service.

When an enterprise interconnects a set of nodes, all under its administrative control, through a LAN network, that is termed an Intranet^[2]. When the interconnected nodes are under multiple administrative authorities but are hidden from the public Internet, the resulting set of nodes is called an extranet. A user organization can manage both intranets and extranets itself, or negotiate a service as a contracted (and usually customized) offering from an IP service provider. In the latter case, the user organization contracts for layer 3 services — much as it may contract for layer 1 services such as dedicated lines, or multiplexed layer 2 services such as frame relay.

The IETF distinguishes between provider-provisioned and customer-provisioned VPNs ^[3]. Just as an interconnected set of providers can supply conventional WAN services, so a single service provider can supply provider-provisioned VPNs (PPVPNs), presenting a common point-of-contact to the user organization.

Routing

Tunneling protocols can be used in a point-to-point topology that would generally not be considered a VPN, because a VPN is expected to support arbitrary and changing sets of network nodes. Since most router implementations support software-defined tunnel interface, customer-provisioned VPNs often comprise simply a set of tunnels over which conventional routing protocols run. PPVPNs, however, need to support the coexistence of multiple VPNs, hidden from one another, but operated by the same service provider.

Building blocks

Depending on whether the PPVPN runs in layer 2 or layer 3, the building blocks described below may be L2 only, L3 only, or combinations of the two. MPLS functionality blurs the L2-L3 identity.

While RFC 4026 generalized these terms to cover L2 and L3 VPNs, they were introduced in RFC 2547. ^[4]

Customer edge device (CE)

In general, a CE is a device, physically at the customer premises, that provides access to the PPVPN service. Some implementations treat it purely as a demarcation point between provider and customer

responsibility, while others allow customers to configure it.

Provider edge device (PE)

A PE is a device or set of devices, at the edge of the provider network, which provides the provider's view of the customer site. PEs are aware of the VPNs that connect through them, and which maintain VPN state.

Provider device (P)

A P device operates inside the provider's core network, and does not directly interface to any customer endpoint. It might, for example, provide routing for many provider-operated tunnels that belong to different customers' PPVPNs. While the P device is a key part of implementing PPVPNs, it is not itself VPN-aware and does not maintain VPN state. Its principal role is allowing the service provider to scale its PPVPN offerings, as, for example, by acting as an aggregation point for multiple PEs. P-to-P connections, in such a role, often are high-capacity optical links between major locations of provide.

User-visible PPVPN services

This section deals with the types of VPN currently considered active in the IETF; some historical names were replaced by these terms.

Layer 1 services

Virtual private wire and private line services (VPWS and VPLS)

In both of these services, the provider does not offer a full routed or bridged network, but components from which the customer can build customer-administered networks. VPWS are point-to-point while VPLS can be point-to-multipoint. They can be Layer 1 emulated circuits with no data link structure.

The customer determines the overall customer VPN service, which also can involve routing, bridging, or host network elements.

An unfortunate acronym confusion can occur between Virtual Private Line Service and Virtual Private LAN Service; the context should make it clear whether "VPLS" means the layer 1 virtual private line or the layer 2 virtual private LAN.

Layer 2 services

Virtual LAN

A Layer 2 technique that allows for the coexistence of multiple LAN broadcast domains, interconnected via trunks using the IEEE 802.1Q trunking protocol. Other trunking protocols have been used but have become obsolete, including Inter-Switch Link (ISL), IEEE 802.10 (originally a security protocol but a subset was introduced for trunking), and ATM LAN Emulation (LANE).

Virtual private LAN service (VPLS)

Developed by IEEE, VLANs allow multiple tagged LANs to share common trunking. VLANs frequently comprise only customer-owned facilities. The former is a layer 1 technology that supports emulation of both point-to-point and point-to-multipoint topologies. The method discussed here extends Layer 2 technologies such as 802.1d and 802.1q LAN trunking to run over transports such as Metro Ethernet.

As used in this context, a VPLS is a Layer 2 PPVPN, rather than a private line, emulating the full functionality of a traditional Local Area Network (LAN). From a user standpoint, a VPLS makes it possible to interconnect several LAN segments over a packet-switched, or optical, provider core; a core transparent to the user, making the remote LAN segments behave as one single LAN.

In a VPLS, the provider network emulates a learning bridge, which optionally may include VLAN service.

Pseudo wire (PW)

PW is similar to VPWS, but it can provide different L2 protocols at both ends. Typically, its interface is a WAN protocol such as ATM or Frame Relay. In contrast, when aiming to provide the appearance of a LAN contiguous between two or more locations, the Virtual Private LAN service or IPLS would be appropriate.

IP-only LAN-like service (IPLS)

A subset of VPLS, the CE devices must have L3 capabilities; the IPLS presents packets rather than frames. It may support IPv4 or IPv6.

L3 PPVPN architectures

This section discusses the main architectures for PPVPNs, one where the PE disambiguates duplicate addresses in a single routing instance, and the other, virtual router, in which the PE contains a virtual router instance per VPN. The former approach, and its variants, have gained the most attention.

One of the challenges of PPVPNs involves different customers using the same address space, especially the IPv4 private address space^[5]. The provider must be able to disambiguate overlapping addresses in the multiple customers' PPVPNs.

BGP/MPLS PPVPN

In the method defined by RFC 2547, BGP extensions advertise routes in the IPv4 VPN address family, which are of the form of 12-byte strings, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. RDs disambiguate otherwise duplicate addresses in the same PE.

PEs understand the topology of each VPN, which are interconnected with MPLS tunnels, either directly or via P routers. In MPLS terminology, the P routers are Label Switch Routers without awareness of VPNs.

Virtual router PPVPN

The Virtual Router architecture ^[6], as opposed to BGP/MPLS techniques, requires no modification to existing routing protocols such as BGP. By the provisioning of logically independent routing domains, the customer operating a VPN is completely responsible for the address space. In the various MPLS tunnels, the different PPVPNs are disambiguated by their label, but do not need routing distinguishers.

Virtual router architectures do not need to disambiguate addresses, because rather than a PE router having awareness of all the PPVPNs, the PE contains multiple virtual router instances, which belong to one and only one VPN.

Categorizing VPN security models

From the security standpoint, VPNs either trust the underlying delivery network, or must enforce security with mechanisms in the VPN itself. Unless the trusted delivery network runs only among physically secure sites, both trusted and secure models need an authentication mechanism for users to gain access to the VPN.

Some ISPs as of 2009 offer managed VPN service for business customers who want the security and convenience of a VPN but prefer not to undertake administering a VPN server themselves. Managed VPNs go beyond PPVPN scope, and are a contracted security solution that can reach into hosts. In addition to providing remote workers with secure access to their employer's internal network, other security and management services are sometimes included as part of the package. Examples include keeping anti-virus and anti-spyware programs updated on each client's computer.

Authentication before VPN connection

A known trusted user, sometimes only when using trusted devices, can be provided with appropriate security privileges to access resources not available to general users. Servers may also need to authenticate themselves to join the VPN.

A wide variety of authentication mechanisms exist. VPNs may implemented authentication in devices including firewalls, access gateways, and others. They may use passwords, biometrics, or cryptographic methods. Strong authentication involves combining cryptography with another authentication mechanism. The authentication mechanism may require explicit user action, or may be embedded in the VPN client or the workstation.

Trusted delivery networks

Trusted VPNs (sometimes referred to APNs - *Actual Private Networks*) do not use cryptographic tunneling, and instead rely on the security of a single provider's network to protect the traffic. In a sense, they elaborate on traditional network- and system-administration work.

- Multi-Protocol Label Switching (MPLS) is often used to overlay VPNs, often with quality-of-service control over a trusted delivery network.
- Layer 2 Tunneling Protocol (L2TP)^[7] which is a standards-based replacement, and a compromise taking the good features from each, for two proprietary VPN protocols: Cisco's Layer 2 Forwarding (L2F)^[8] (obsolete as of 2009) and Microsoft's Point-to-Point Tunneling Protocol (PPTP)^[9].

Security mechanisms

Secure VPNs use cryptographic tunneling protocols to provide the intended confidentiality (blocking snooping and thus Packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy. When properly chosen, implemented, and operated, such techniques can provide secure communications over unsecured networks.

Secure VPN protocols include the following:

- IPsec (IP security) - commonly used over IPv4, and a "standard option" in IPv6.
- SSL/TLS, used either for tunneling the entire network stack, as in the OpenVPN project, or for securing what is, essentially, a web proxy is called SSL VPN. SSL, though a framework more often associated with e-commerce, has been built-upon by a number of vendors to provide remote access VPN capabilities. A major practical advantage of an SSL VPN is that it can be accessed from the locations that restrict external access to SSL-based e-commerce websites only, thereby preventing VPN connectivity using IPsec protocols. SSL-based VPNs are vulnerable to trivial Denial of Service attacks mounted against their TCP connections because latter are inherently unauthenticated.
- OpenVPN, an open standard VPN. A variation of SSL VPN, it can run over UDP. Clients and servers are available for all major operating systems.
- DTLS, used by Cisco for a next generation VPN product called Cisco AnyConnect VPN. DTLS solves the issues found when tunneling TCP over TCP as is the case with SSL/TLS
- SSTP from Microsoft introduced in Windows Vista Service Pack 1. SSTP tunnels PPP or L2TP traffic through an SSL 3.0 channel.
- L2TPv3 (Layer 2 Tunneling Protocol version 3), a new release.
- VPN Quarantine. The client machine at the end of a VPN could be a threat and a source of attack; this has no connection with VPN design and most VPN providers leave it to system administration to secure. There are solutions that provide VPN Quarantine services which run end point checks on the remote client while the client is kept in a quarantine zone until healthy. Microsoft ISA Server 2004/2006 together with VPN-Q 2006 from Winfrasoft or an application called QSS (Quarantine Security Suite) provide this functionality.
- MPVPN (Multi Path Virtual Private Network). Ragula Systems Development Company owns the registered trademark "MPVPN".^[10]
- Cisco VPN, a proprietary VPN used by many Cisco hardware devices. Proprietary clients exist for all platforms; open-source clients also exist.

Security and mobility

Mobile VPNs are VPNs for mobile and wireless users. They apply standards-based authentication and encryption technologies to secure communications with mobile devices and to protect networks from unauthorized users. Designed for wireless environments, Mobile VPNs provide an access solution for mobile users who require secure access to information and applications over a variety of wired and wireless networks. Mobile VPNs allow users to roam seamlessly across IP-based networks and in and out of wireless-coverage areas without losing application sessions or dropping the secure VPN session. For instance, highway patrol officers require access to mission-critical applications as they travel between different subnets of a mobile network, much as a cellular radio has to hand off its link to repeaters at different cell towers.

The Host Identity Protocol (HIP), under study by the Internet Engineering Task Force, is designed to

support mobility of hosts by separating the role of IP addresses for host identification from their locator functionality in an IP network. With HIP a mobile host maintains its logical connections established via the host identity identifier while associating with different IP addresses when roaming between access networks.

See also

- IPsec
- Transport Layer Security
- DTLS
- Opportunistic encryption
- Host Identity Protocol
- Split tunneling
- Intranet
- Local Area Network
- OpenVPN, an open source VPN program
- n2n, a Free Software peer-to-peer VPN program
- Netsentron, a proprietary appliance

References

1. ^ IP Based Virtual Private Networks,RFC 2764, B. Gleeson *et al.*,February2000
2. ^ Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN),RFC3809, A. Nagarajan,June 2004
3. ^ Provider Provisioned Virtual Private Network (VPN) Terminology,RFC4026, L. Andersson and T. Madsen,March 2005
4. ^ E. Rosen & Y. Rekhter (March 1999). "RFC 2547 BGP/MPLS VPNs". Internet Engineering Task Force (IETF). <http://www.ietf.org/rfc/rfc2547.txt>.
5. ^ Address Allocation for Private Internets,RFC 1918, Y. Rekhter *et al.*,February 1996
6. ^ A Core MPLS IP VPN Architecture,RFC 2918, K. Muthukrishnan & A. Malis, September 2000
7. ^ Layer Two Tunneling Protocol "L2TP",RFC 2661, W. Townsley *et al.*,August 1999
8. ^ IP Based Virtual Private Networks,RFC 2341, A. Valencia *et al.*, May 1998
9. ^ Point-to-Point Tunneling Protocol (PPTP),RFC 2637, K. Hamzeh *et al.*,July 1999
10. ^ Trademark Applications and Registrations Retrieval (TARR)

External links

- JANET UK "Different Flavours of VPN: Technology and Applications"
- VPN Encryption
- Virtual Private Network Consortium - a trade association for VPN vendors
- Microsoft TechNet VPN Resources
- ZeroShell, a small Linux distribution which can act as VPN box for LAN-to-LAN and host-to-LAN VPNs
- Tutorial using the built-in Windows PPTP VPN function
- "How Virtual Private Networks Work": a basic tutorial
- OpenVPN: a free cross-platform VPN server/client

Retrieved from "http://en.wikipedia.org/wiki/Virtual_private_network"

Categories: VPN | Network architecture | Computer network security | Internet privacy | Crypto-

anarchism

Hidden categories: Cleanup from January 2009 | All pages needing cleanup | Wikipedia articles needing clarification from January 2009 | Wikipedia articles needing clarification from February 2009 | Articles containing potentially dated statements from 2009 | All articles containing potentially dated statements | All articles with unsourced statements | Articles with unsourced statements since October 2007

- This page was last modified on 28 March 2009, at 15:47.
 - All text is available under the terms of the GNU Free Documentation License. (See **Copyrights** for details.)
- Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3) tax-deductible nonprofit charity.